



Pension Benefit Guaranty Corporation
Office of Inspector General
Audit Report

**Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's Fiscal
Year 2010 and 2009 Financial Statements Audit**

November 12, 2010

AUD-2011-3/FA-10-69-2



Pension Benefit Guaranty Corporation

Office of Inspector General

1200 K Street, N.W., Washington, D.C. 20005-4026

November 12, 2010

To: Joshua Gotbaum
Director
Pension Benefit Guaranty Corporation

Patricia Kelly
Chief Financial Officer

From: Joseph A. Marchowsky *Joseph A. Marchowsky*
Assistant Inspector General for Audit

Subject: Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2010 and 2009 Financial Statements Audit (AUD-2011-3 / FA-10-69-2)

I am pleased to transmit the attached report prepared by Clifton Gunderson LLP resulting from their audit of the PBGC Fiscal Year 2010 and 2009 Financial Statements. The purpose of this report is to provide more detailed discussions of the specifics underlying the significant deficiencies and material weakness reported in the internal control section of the combined Independent Auditor's Report dated November 12, 2010 (AUD-2011-2/FA-10-69-1). The attached management response to a draft of this report indicates management's agreement with each recommendation and their commitment to addressing the recommendations contained in the report and to remediating the associated material weakness.

We would like to take this opportunity to express our appreciation for the overall cooperation that Clifton Gunderson auditors and we received while performing the audit.

Attachment

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2010 and 2009 Financial Statements

Audit Report AUD-2011-3 / FA-10-69-2

Contents

Section I: Independent Auditor's Report

Section II: Management Comments

Acronyms

BPD	Bureau of Public Debt
C&A	Certification and Accreditation
CAP	Corrective Action Plan
CFS	Consolidated Financial System
COOP	Continuity of Operations Program
EDM	Enterprise Data Model
ELAN	Enterprise Local Area Network
FIPS PUB	Federal Information Processing Standards Publication
FMFIA	Federal Managers' Financial Integrity Act of 1982
FY	Fiscal Year
IAA	Interagency Agreement
IAH	Information Assurance Handbook
IPVFB	Integrated Present Value of Future Benefits
ISO	Information System Owner
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAS	Premium Accounting System
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
PPS	Premium and Practitioner System
PRISM	Participant Records Information Systems Management
RTM	Requirements Traceability Matrix
TAS	Trust Accounting System

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2010 and 2009 Financial Statements

Audit Report AUD-2011-3 / FA-10-69-2

Section I

Independent Auditor's Report

Pension Benefit Guaranty Corporation

To the Board of Directors, Management,
and Inspector General of the
Pension Benefit Guaranty Corporation
Washington, DC

We have audited the financial statements of the Pension Benefit Guaranty Corporation (PBGC) as of and for the year ended September 30, 2010, and have examined management's assertion included in PBGC's Annual Report about the effectiveness of the internal control over financial reporting (including safeguarding assets) and PBGC's compliance with certain provisions of laws, regulations, and other matters, and have issued our combined report thereon dated November 12, 2010 (see OIG report AUD-2011-2/FA-10-69-1).

We conducted our audit and examination in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*, issued by the Comptroller General of the United States; attestation standards established by the American Institute of Certified Public Accountants; and Office of Management and Budget (OMB) audit guidance.

The purpose of this report is to provide more detailed discussions of the specifics underlying the material weakness reported in the internal control section of our combined report on PBGC's fiscal year (FY) 2010 financial statements. As reported in our combined report on PBGC's FY 2010 financial statements, we identified certain deficiencies in internal control that we consider significant deficiencies, which combined constitute a material weakness.

Summary

PBGC protects the pensions of approximately 44 million workers and retirees in more than 27,500 private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on information technology (IT). Internal controls over these operations are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

Our review of IT controls covered general and selected business process application controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer systems. They include entity-wide security management, access controls, configuration management, segregation of duties and contingency planning controls. Business process application controls are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

Our review also included the integration of financial management systems to ensure effective and efficient interrelationships. These interrelationships include common data elements, common transaction processing, consistent internal controls, and transaction entry.

PBGC's systemic security control weaknesses and the lack of an integrated financial management system continued to pose an increasing and substantial risk to PBGC's ability to carry out its mission during FY 2010. PBGC's key decision makers are acutely aware of the challenges facing the Corporation in addressing fundamental weaknesses in its IT infrastructure and environment. Management has therefore taken a multiyear approach to correct these deficiencies at the root cause level. However, in past years, communication between PBGC's key decision makers did not convey the urgent need for decisive strategic decisions to correct fundamental weaknesses in PBGC's IT infrastructure and environment. Strategic IT decisions did not address these deficiencies, and significant weaknesses identified in prior years, continued to persist.

PBGC's decentralized approach to system development and configuration management has exacerbated control weaknesses and encouraged inconsistency in implementing strong technical controls and best practices. The influx of 620 plans for over 800,000 participants from 2002-2005, contributed to PBGC's disjointed IT development and implementation strategy. The mandate to meet PBGC's mission objectives by implementing technologies to receive the influx of plans superseded proper enterprise planning and IT security controls. The result was a series of stovepipe solutions built upon unplanned and poorly integrated heterogeneous technologies with varying levels of obsolescence.

The Corporation has now embarked on a more coherent strategy and cost effective approach to resolving and correcting these fundamental IT weaknesses. PBGC has developed and is implementing a multi-year corrective action plan (CAP) to address security issues at the root cause level. However, PBGC management realizes these weaknesses will continue to pose a threat to its environment for several years while corrective actions are being implemented. PBGC will need to implement interim corrective actions to ensure fundamental security weaknesses do not worsen as the CAP is being implemented.

PBGC has entered into an interagency agreement (IAA) with the Bureau of Public Debt (BPD) of the Department of the Treasury to assist PBGC in revising and strengthening its security management program and certification and accreditation (C&A) process. The multi-year CAP includes the implementation of a more effective C&A process, addressing fundamental security weaknesses and initiating an IT infrastructure modernization program. In FY 2010, PBGC procured and implemented new hardware in its infrastructure, as it works towards modernization of its IT infrastructure. Additional future actions include completing PBGC's Enterprise Architecture segment.

Our current year audit work continued to find deficiencies in the areas of security management, access controls, configuration management, and segregation of duties. Control deficiencies were also found in policy administration, and the C&As of major applications and general support systems. An effective entity-wide security management program requires a coherent strategy for the architecture of the IT infrastructure, and the deployment of systems. The implementation of a coherent strategy provides the basis and foundation for the consistent application of policy, controls, and best practices. PBGC first needs to develop and implement a framework to improve their security posture. This framework will require time for effective control processes to mature.

Based on our findings, we are reporting that significant deficiencies in the following areas constitute a material weakness for FY 2010:

1. Entity-wide security program planning and management
2. Access controls and configuration management
3. Integrated financial management systems

Detailed findings and recommendations follow.

1. Entity-wide Security Program Planning and Management

During FY 2010, PBGC made strategic decisions to develop and implement a multi-year CAP to address fundamental weaknesses in its entity-wide security program planning and management. PBGC entered into an IAA for the services of the BPD to assist the Corporation in reassessing its security program and developing a framework for implementing a more coherent strategy for correcting fundamental IT security weaknesses at the root cause level. However, in past years, communication between PBGC's key decision makers did not convey the urgent need for decisive strategic decisions to correct fundamental weaknesses in PBGC's IT infrastructure and environment. Strategic IT decisions did not address these deficiencies, and significant weaknesses continued to persist. PBGC management realizes these weaknesses will continue to pose a threat to its environment for several years while corrective actions are being implemented.

PBGC abandoned its C&A documentation and is working with BPD to revise and strengthen its C&A process to ensure security weaknesses are addressed at the root cause level. PBGC did not conduct any C&As in FY 2010. The Corporation has implemented a multi-year plan to correct its C&As.

In prior years, PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. These deficiencies, which continue to persist, prevent PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. The specific weaknesses we found that contributed to the material weakness and our recommendations to correct them are as follows:

- PBGC identified 65 common security controls for the 17 National Institute of Standards and Technology (NIST) special publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, security control families. Of the 65 common security controls tested by PBGC in FY 2008, only four controls were properly designed and operating effectively. PBGC did not continue its implementation of common controls in FY 2009 and FY 2010. Weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications adversely affected its ability to effectively implement common security controls across its systems and applications. Without full development and implementation, security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions lead to insufficient protection of sensitive or critical resources or disproportionately high expenditures for controls. Consequently, PBGC has not completed and confirmed the design, implementation, and operating effectiveness of its common security controls. Without testing control processes, management cannot have confidence that the controls were implemented.

Recommendations:

- Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses. **(OIG Control # FS-09-01)**
- Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. **(OIG Control # FS-08-01)**
- Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control # FS-09-02)**
- PBGC's process for the completion of C&A packages in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, is ineffective. Fundamental weaknesses in PBGC's infrastructure architecture and design do not support the C&A of its information systems. Furthermore, PBGC's information systems employ obsolete and antiquated technologies that pose additional risk to the availability of financially significant systems. PBGC abandoned its C&A packages and is working with BPD to revise and strengthen its C&A process to ensure security weaknesses are addressed at the root cause level. PBGC did not conduct C&As in FY 2010. The Corporation has implemented a multi-year plan to correct its C&As.

In FY 2009, PBGC asserted the completion of 13 C&A packages for its major applications and general support systems. However, our review identified significant deficiencies in access controls and configuration management. PBGC's quality control review of the C&A packages did not correct specific issues we identified in FY 2009. In addition, PBGC's oversight of contractor performance during the C&A process was inadequate. The C&A packages were deficient in their quality, accuracy, and consistency.

Our review of the C&A packages noted the following quality control weaknesses, each of which had been identified in our prior year audit:

- Limited documentation of test results, a condition that prevented third-party reviewers from re-performing, and thus validating, the tests.
- Deficiencies not included in the Plan of Action and Milestones.
- Documentation that did not support conclusions reached or test results.
- Inconsistencies or apparent errors and/or omissions in work performed.
- Information in the system boundaries section of the risk assessment conflicted with the listing of external connections.
- Minor applications identified in Security Control Worksheet, but not documented in the Risk Assessment.

Without management oversight and accountability of contractor's performance, management may accept work that does not meet Federal criteria. Such practices may lead to fraud, waste, or abuse; and to insufficient protection of sensitive or critical resources. In addition, projects may exceed approved budget if rework is required. Without monitoring contractor performance and performing a quality review of deliverables, management cannot have confidence in the work performed.

PBGC did not provide an inventory of its major applications and general support systems in FY 2010. In FY 2009, management provided three conflicting inventory lists of major applications and general support systems. Some systems considered major on one inventory list, were considered minor on the others. We could not determine management's assertion concerning the inventory of its major applications and general support systems. Because of the contradictory information provided, we could not determine which of these lists should be considered as management's assertion concerning the inventory of its major applications and general support systems. Therefore, we could not determine which major applications and general support systems require C&A.

The risk exists that systems could be certified, accredited, and receive an authorization to operate without the assurance that complete and accurate results are obtained in executing the C&A process. In addition, issues identified or missed because of inaccurate or incomplete work performed will impact the corrective action required along with the resource commitment needed to complete the intended action. PBGC did not obtain a waiver from the OMB, allowing conditional authorization of its systems, as cited in OIG report *Authorization to Operate PBGC Information Systems* (AUD-2010-8 / IT-09-70), issued August 19, 2010.

PBGC does not have reasonable assurance regarding the confidentiality, integrity, and availability of its information systems.

Recommendations:

- Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies. **(OIG Control # FS-09-03)**
- Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control # FS-09-04)**
- Implement an effective review process to validate the completion of the C&A packages for all major applications and general support systems. The review should not be performed by an individual associated with the performance of the C&A, or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control # FS-08-02)**
- Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the C&A process. **(OIG Control # FS-09-05)**
- Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the certification and review process. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control # FS-09-06)**

- Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC Office of IT (OIT) operations. **(OIG Control # FS-09-07)**
- Implement an independent and effective review process to validate the completion of the C&A packages for all applications and general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control # FS-08-03)**
- Implement robust and rigorous review procedures to verify that future contracts for the C&A of PBGC's systems clearly outline expectations and deliverables in the statement of work. **(OIG Control # FS-09-08)**
- Implement a robust and rigorous quality review process to verify contractor C&A deliverables meet the requirements specified in the statement of work. **(OIG Control # FS-09-09)**
- Establish controls to ensure that contract staff tasked with the C&A of PBGC systems have the appropriate knowledge and background to accurately and comprehensively complete the C&A process. **(OIG Control # FS-09-10)**
- Implement a robust and rigorous process to verify compliance with PBGC's policy on contractor management throughout the C&A lifecycle. **(OIG Control # FS-09-11)**
- Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for Security Awareness training. PBGC currently has a cumbersome and error-prone manual process to account for personnel who had completed security awareness training. The process is ineffective and limits PBGC's ability to ensure that all required personnel have completed security awareness training. In FY 2009, PBGC developed role-based training programs to disseminate its Information Assurance Handbook (IAH) policies and procedures to information system owners (ISOs), system administrators, and project managers. During our FY 2009 review, we noted that PBGC could not verify and validate whether all required personnel had completed the Information Security Awareness Training. Some project managers, ISOs and system administrators did not attend the risk management role-based training. The Contingency Plan Specialist was not aware of IAH guidance on required annual contingency training. Fifteen PBGC officials with Continuity of Operations Program (COOP) responsibilities did not attend required annual contingency training.

PBGC changed its approach for its CAP process by placing more emphasis on correcting the root cause. This approach has resulted in completion dates being revised, and a multi-year approach to correct weaknesses noted above. Management indicated, in their CAP, that this finding would be remediated by September 30, 2011.

In the interim, lack of security awareness can lead to increased risk of security breaches and exposure to fraud. Controls may not be placed in operation as mandated by PBGC policies.

Recommendation:

- Develop and implement a process to enforce the dissemination and awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04)**
- OIT and system owners (i.e. business owners) have not established and documented service level agreements that include metrics on OIT services required to meet business goals. PBGC is in the process of completing the development and distribution of measurable services provided to the business owners by the OIT.

Recommendation:

- Establish, document, and publish measurable services that OIT provides to the Corporation, that are acceptable to all ISOs. **(OIG Control # FS-07-06)**
- PBGC's benefit payments service provider (service provider) implemented a security operations center (SOC) outside of the United States (US), which will have some responsibility for monitoring security related events associated with the Pension Lump Sum (PLUS) application and components of its system boundary. The service provider did not provide PBGC with adequate advance notice to assess the security impact to the PLUS application on the change in environment before going operational. Furthermore, PBGC was not provided adequate time to assess risks to its systems and implement mitigating controls to ensure compliance with the PBGC's policies and procedures. As a result, PBGC has not assessed the security impact of the change in environment.

Recommendation:

- Develop and implement an immediate plan of action to address the potential security risk posed by locating the Security Operations Center outside of the US. **(OIG Control # FS-10-01)**
- Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and FISMA. **(OIG Control #FS-10-02)**
- PBGC has not executed an interconnection security agreement (ISA) or memorandum of understanding (MOU) between external organizations whose systems interconnect with PBGC's systems.

PBGC is in the process of planning and documenting security agreements for interconnection with external organizations' systems. In the absence of an ISA and MOU, either party (PBGC or external system owner) may be unfamiliar with the technical requirements of the interconnection and details that may be required to provide an overall security for systems that are interconnected.

Recommendation:

- Develop and implement an ISA and MOU with external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03)**

2. Access Controls and Configuration Management

Although access controls and configuration management controls are an integral part of an effective information security management program, access controls remain a systemic problem throughout PBGC. PBGC's decentralized approach to system development, system deployments, and configuration management created an environment that lacks a cohesive structure in which to implement controls and best practices. Weaknesses in the IT environment contributed significantly to deficiencies in system configuration, segregation of duties, role-based access controls, and monitoring. Furthermore, PBGC's information systems are overlapping and duplicative, employing obsolete and antiquated technologies that are costly to maintain. The state of PBGC's IT environment led to increased IT staffing needs, manual workarounds, reconciliations, extensive manipulation, and excessive manual processing that have been ineffective in providing adequate compensating controls to mitigate system control weaknesses. For example, the Financial Reporting and Account Analysis Group manually records present value of future benefits liabilities for single employer and multiemployer programs in the Consolidated Financial System (CFS), and the Financial Operations Department manually records Premium Income, Premium Receivables, and Unearned Premiums in CFS.

Access controls should be in place to consistently limit, detect inappropriate access to computer resources (data, equipment, and facilities), or monitor access to computer programs, data, equipment, and facilities. These controls protect against unauthorized modification, disclosure, loss, or impairment. Such controls include both logical and physical security controls to ensure that Federal employees and contractors will be given only the access privileges necessary to perform business functions. Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum access controls for Federal systems. FIPS PUB 200 requires PBGC's ISOs to limit information system access to authorized users.

Industry best practices, NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, and other Federal guidance recognize the importance of configuration management when developing and maintaining a system or network. Through configuration management, the composition of a system is formally defined and tracked to ensure that an unauthorized change is not introduced. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system, on an ongoing basis, is an essential aspect of maintaining the security posture. An effective entity-wide configuration management and control policy and associated procedures are essential to ensuring adequate consideration of the potential security impact of specific changes to an information system. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the entity and subsequently controlling and maintaining an accurate inventory of any changes to the system.

Inappropriate access and configuration management controls do not provide PBGC with sufficient assurance that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

PBGC management realizes these weaknesses will continue to pose a threat to its environment for several years while corrective actions are being implemented. PBGC developed a CAP that is a three to five year holistic approach starting in FY 2010. The CAP has been broken into several process families to address the underlying root causes of the findings. The specific weaknesses we continued to find that contributed to the material weakness and our recommendations to correct them are as follows:

- PBGC's configuration management controls are labor intensive and ineffective. Weaknesses in the design of PBGC's infrastructure and deployment strategy for systems and applications created an environment where strong technical controls and best practices cannot be effectively implemented. Configuration management controls are therefore not consistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server configurations; therefore, management cannot rely on results obtained in the development or test environments prior to deployment in production. Overall, the PBGC environment suffers from inadequate configuration, roles, privileges, logging, monitoring, file permissions, and operating system access.

PBGC's infrastructure does not adequately segregate the production, development and testing environments. The current environment does not provide adequate controls in which to implement an effective application development and change control program.

Significant weaknesses noted in configuration management continued in FY 2010, include the following:

- Sensitive program scripts and utilities, open directories, and unsafe services accounts were not restricted.
- Unnecessary network services and duplicate groups with privileged system access were not removed.
- Baseline security reports were not being created and reviewed.
- Inappropriate configuration/ownership of critical files, directories, and permissions.
- The root account could be logged into from multiple virtual consoles.
- The method in which database replication was taking place from headquarters to the COOP installation is lacking in functionality and completeness, and would require a significant amount of subject matter expert manual intervention to failback, in the event of an actual system failure.
- Developers had access to sensitive information in production by having direct development access to production systems via a database link.
- Development and test databases have database links directly connected to the production database. This configuration of database links produces an inefficient, difficult to manage, non-scalable Oracle database solution.
- The IT System Life Cycle Methodology is not consistently implemented across all projects within PBGC. We reviewed the Product Quality Assurance audit summary of the HP Service Manager 7 software implementation and noted that various critical components were lacking such as:
 - Weaknesses noted in the approval, configuration management and change control processes.
 - Failure to obtain approval signatures on key documents and test artifacts.
 - Incomplete Requirements Traceability Matrix (RTM).
 - Failure to update the RTM resulting in lack of traceability between the requirements and the test cases.

- Lack of evidence that key test activities were conducted in the test environment as planned.
- Backout plans for reversing system changes in case of an unexpected situation are not consistently documented.

Controls are not in place to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected. Applications and critical business processes may not be restored in a timely manner in the event of a true disaster.

Recommendations:

- Develop and implement procedures and processes for the consistent implementation of common configuration management controls to minimize security weaknesses in general support systems. **(OIG Control # FS-07-07)**
- Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control # FS-09-12)**
- Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # FS-09-13)**
- Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control # FS-09-14)**
- Ensure test, development and production databases are appropriately segregated to protect sensitive information and fully utilized to increase system performance. **(OIG Control # FS-09-15)**
- Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control # FS-09-16)**
- PBGC's policies and practices have not effectively restricted the addition of unnecessary and generic accounts to systems in production. Consequently, the number of unnecessary and generic accounts grew over the years. PBGC management has not determined if the removal of all legacy generic accounts would disrupt production activities.

Failure to identify and remove unnecessary accounts from the system could result in PBGC's systems being at an increased risk for unauthorized access/modification/deletion of sensitive system and/or participant information.

Recommendation:

- Continue to remove unnecessary user and/or generic accounts. **(OIG Control # FS-07-08)**
- Controls are not consistently implemented to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. PBGC does not have a coherent strategy for enforcing segregation of duties through strong technical controls in its applications and general support systems. PBGC's decentralized approach to system development and configuration management has exacerbated inconsistency and control weaknesses in implementing strong technical controls to enforce segregation of incompatible duties.

Incompatible duties and improper password management increase the potential risk of fraud, errors and omissions.

Recommendations:

- Consistently implement controls to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. **(OIG Control # FS-07-09)**
- Assess the risk associated with lacking segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. **(OIG Control # FS-09-17)**
- Developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of the application, the circumvention of critical controls, and unnecessary access to sensitive data. Weaknesses in the design of PBGC's infrastructure and deployment strategy for legacy systems and applications created an environment where developers have unrestricted access to production. PBGC has not developed and implemented adequate compensating controls to restrict developer's access to production. PBGC has not fully resolved infrastructure design issues, nor have they developed and implemented a coherent program to manage and maintain legacy applications.

Failure to appropriately restrict privileged access to the production environment could result in unauthorized access/modification/deletion to sensitive system and/or participant information and the release of harmful code into the production environment.

Recommendations:

- Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10)**
- Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed. **(OIG Control # FS-09-18)**

- Controls are not consistently applied to ensure that authentication parameters for general support systems (e.g. Novell, Windows, SUN Solaris, Oracle, etc.) and applications comply with the IAH. PBGC's decentralized approach to system development and configuration management has made it particularly difficult to implement consistent technical controls across PBGC's many systems, platforms, and applications.

Failure to follow secure build standards and reassign or remove unowned user files provides internal and external attackers additional paths into PBGC's systems and could result in an increased risk of unauthorized access, modification, or deletion of sensitive system and participant information. These control weaknesses increase the risk for fraud, waste and abuse.

Recommendations:

- Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications comply with the IAH. **(OIG Control # FS-07-11)**
- Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control # FS-09-19)**
- PBGC is still in the process of identifying dependencies between databases, applications, and operating systems in order to fully implement controls to lock out and remove inactive and dormant accounts. However, there are still some PBGC systems that have not implemented these controls. PBGC's configuration management weaknesses have contributed significantly to its inability to effectively implement controls to ensure the consistent removal and locking out of generic or dormant accounts.

Without full development and implementation of security controls, the lack of an effective policy addressing lock out, inactive accounts, and dormant accounts provides another control weakness that could be exploited and compromise the integrity, confidentiality and availability of PBGC's systems and applications.

Recommendation:

- For the remaining systems, apply controls to lock out and remove inactive and dormant accounts after a specified period in accordance with the IAH. **(OIG Control # FS-07-12)**
- The OIT recertification process is incomplete and only addresses generic and service accounts; it does not include all user and system accounts. In addition, the Recertification of User Access Process, version 1.2, does not explicitly state that all accounts (e.g. user, system, and service) across all platforms and applications will be recertified annually. PBGC's infrastructure design and configuration management weaknesses have contributed significantly to its inability to effectively implement controls to recertify all user and system accounts.

Unauthorized users could gain access to PBGC's data and personally identifiable information (PII). Without periodic recertification of accounts (user, generic, service and system) management does not have adequate assurance that only current authorized users have access to PBGC resources.

Recommendation:

- Complete the implementation of the recertification process for all user and system accounts. Continue to perform annual recertification and include all PBGC's accounts (e.g. user, generic, service, and systems accounts) for general support systems and major applications. **(OIG Control # FS-07-13)**
- Vulnerabilities found in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. These PBGC system vulnerabilities are caused by an ineffective deployment strategy in the development, test, and production environments. Ineffective system deployments have resulted in an environment that is in disarray.

Security control weaknesses and vulnerabilities in key databases were not mitigated, and adversely impacted the security and integrity of PBGC's development, test, and production environments. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur, undetected.

Recommendations:

- Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control # FS-07-14)**
- Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control # FS-09-20)**
- Access request authorizations were not appropriately documented. PBGC has not fully implemented controls to ensure Enterprise Local Area Network forms are properly documented and maintained.

Failure to ensure proper authorization may expose PBGC's systems to inadequate segregation of incompatible duties and unauthorized users having access to PBGC data and PII.

Recommendation:

- Ensure that adequate documentation of access authorization is maintained by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control # FS-07-15)**
- PBGC lacks an effective process to track contractors throughout their employment at PBGC, including appropriate notifications of start dates and separation. Management reported that policies and procedures, to include PBGC directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, have

not been updated to provide effective enforcement of controls designed to track entrance and separation of all Federal and contract employees.

Without full development and implementation, security controls are inadequate to prevent contractors from having unauthorized access to PBGC's systems, applications, and facilities.

Recommendations:

- Update and enforce directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. **(OIG Control # FS-07-16)**
- Periodic logging and monitoring of security-related events for PBGC's applications were inadequate for CFS, PAS, Trust Accounting System (TAS), Participant Records Information Systems Management (PRISM), and Integrated Present Value of Future Benefits (IPVFB) systems. PBGC's IT infrastructure consist of multiple legacy systems and applications (e.g. PAS, TAS, IPVFB, PRISM, GENESIS database, Solaris 8, Oracle 8i, Novell NetWare 5.1, Windows NT, etc.) that do not have a coherent architecture for management and security.

Controls are not in place to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur, undetected.

Recommendation:

- Implement a logging and monitoring process for application security related events and critical system modifications (e.g. CFS, PAS, TAS, PRISM, and IPVFB). **(OIG Control # FS-07-17)**
- The application virtualization/application delivery product Citrix MetaFrame Presentation Server used by PBGC's benefit payments service provider to connect to its benefit payments system, PLUS, reached its end of life date on December 31, 2009. PBGC did not include the Citrix MetaFrame Presentation Server in the system boundary when conducting the C&A of the PLUS application. Although continuous monitoring was implemented, no alerts were provided to PBGC about the application virtualization/application becoming obsolete and the potential security risk to PLUS. Obsolete software may expose PBGC's infrastructure to a security-related vulnerability. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected.

Recommendation:

- Replace the Citrix MetaFrame presentation server. **(OIG Control #FS-10-04)**

- Include the application virtualization/application delivery product used by the benefits payments service provider to access the PLUS application in the system boundary. **(OIG Control # FS-10-05)**
- The TeamConnect application, which replaced the Lotus Notes system in FY 2010, maintains a nightly premium output batch file error log in a .txt file format, which can be edited. Management has not locked down the TeamConnect output file from manipulation. Because the exception log data can be manipulated, the Actuarial database into which the data is being transferred, may be compromised or corrupted. Unresolved inaccuracies between the Corporate Data Management System and the Actuarial Database could result in errors in the amount of contingent liabilities recorded and disclosed in the financial statement.

Recommendation:

- Configure TeamConnect to ensure the integrity of the nightly premium output batch file error log. **(OIG Control # FS-10-06)**

3. Integrated Financial Management Systems

The risk of inaccurate, inconsistent, and redundant data is increased because PBGC lacks a single integrated financial management system. The current system cannot be readily accessed and used by financial and program managers without extensive manipulation, excessive manual processing, and inefficient balancing of reports to reconcile disbursements, collections, and general ledger data.

OMB Circular A-127, *Financial Management Systems*, requires that Federal financial management systems be designed to provide for effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the systems. This Circular states:

The term "single, integrated financial management system" means a unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, processes (manual and automated), procedures, controls and data necessary to carry out financial management functions, manage financial operations of the agency and report on the agency's financial status to central agencies, Congress and the public. Unified means that the systems are planned for and managed together, operated in an integrated fashion, and linked together electronically in an efficient and effective manner to provide agency-wide financial system support necessary to carry out the agency's mission and support the agency's financial management needs.

OMB's Office of Federal Financial Management, formerly the Joint Financial Management Improvement Program, "*Core Financial System Requirements*" document, lists the following integrated financial management system attributes:

- Standard data classifications (definition and formats) established and used for recording financial events.
- Common processes used for processing similar kinds of transactions.

- Internal controls over data entry, transaction processing, and reporting that are applied consistently.
- A system design that eliminates unnecessary duplication of transaction entry.

Because PBGC has not integrated its financial systems, PBGC's ability to accurately and efficiently accumulate and summarize information required for internal and external financial reporting is impacted. Many of the weaknesses included in this report were reported in prior years. The specific weaknesses we found that contributed to the material weakness and our recommendations to correct them are as follows:

Lack of standard data classifications and common data elements:

- PBGC continues to work towards a logical database model (Enterprise Data Model (EDM)). Elements of the EDM include the general ledger, purchases, portfolio management, payroll, investment management, financial institutions, budgeting, accounts receivable, and accounts payable. Until the development and implementation of the EDM is complete, the current systems have no centralized data catalog defining data elements or a common data access method available for current databases.
- The current decentralized database structure may lead to erroneous financial and participant data. For example, the same data elements are required to be reformatted or are used for different purposes across PBGC's various applications.
- The current decentralized database structure may lead to outdated financial or participant data. Because participant data must be reformatted and distributed to multiple PBGC systems, users may be relying on outdated information to make business decisions.

Duplication of transaction entry:

- Probable and multi-employer plan data initially entered into IPVFB must be manually re-entered into a spreadsheet and then manually entered into CFS as adjusting journal entries.
- Plan data initially entered into the Case Management System application must be re-entered into the TAS application's portfolio header.
- Plan contingency listings are determined using data extracted from PAS. However, plans with multiple filings must be manually aggregated before the plans can be classified.
- Plan sponsor data address information must be manually entered into CFS to process refunds.

Obsolete and antiquated technologies:

PBGC's information systems employ obsolete and antiquated technologies that pose additional risk to the availability of financially significant systems. These technologies are unsupported and add to the challenges to integrate PBGC's systems in an IT infrastructure that lacks a cohesive architecture and design.

A Federal agency's ability to effectively and efficiently maintain and modernize its existing IT environment depends primarily on how well it employs certain IT management controls that are embodied in statutory requirements, Federal guidance, and best practices. Among other things, these controls include strategic planning and performance measurement, portfolio-based investment management, human capital management, enterprise architecture (and

supporting segment architecture) development and use, and responsibility and accountability for modernization management.

If managed effectively, IT investments can have a dramatic impact on an organization's performance and accountability. If not correctly managed, they can result in wasteful spending and lost opportunities for achieving mission goals and improving mission performance. PBGC had several false starts in modernizing its systems and applications that have either been abandoned, such as the suspension of work on the PPS to replace PAS, or have been ineffective in leading to the integration of its financially significant systems. Unless PBGC develops and implements a well designed IT architecture and infrastructure to guide and constrain modernization projects, it risks investing time and resources in systems that do not reflect the Corporation's priorities, are not well integrated, are potentially duplicative, and do not optimally support mission operations and performance.

To its credit, PBGC began to develop an overall strategy, but much work remains before the strategy can be completed and implemented. Steps PBGC has taken include the following:

1. PBGC identified all systems that provide data required to prepare the financial statements.
2. PBGC substantially completed the logical database model including standard data definitions and formats to be used throughout the Corporation.
3. PBGC completed alternative analysis studies for Premium Accounting and CFS.

Major work remains to be completed to set the foundation for an integrated financial management system, including the development and implementation of new IT system solutions/functions in accordance with the Financial Management Segment Architecture and strategic system plan.

Recommendation:

- PBGC needs to develop and execute a plan to integrate its financial management systems in accordance with OMB Circular A-127. **(OIG Control # FS-07-18)**

The internal control report recommendations status is presented in Exhibit I.

This report is intended for the information and use of the management and Inspector General of PBGC and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Henderson LLP

Calverton, Maryland
November 12, 2010

EXHIBIT I - Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendations Closed During FY 2010:

Recommendation	Date Closed	Original Report Number
None		

Open Recommendations as of September 30, 2010:

Recommendation	Report
Prior Years'	
FS-07-04	2008-2/FA-0034-2
FS-07-06	2008-2/FA-0034-2
FS-07-07	2008-2/FA-0034-2
FS-07-08	2008-2/FA-0034-2
FS-07-09	2008-2/FA-0034-2
FS-07-10	2008-2/FA-0034-2
FS-07-11	2008-2/FA-0034-2
FS-07-12	2008-2/FA-0034-2
FS-07-13	2008-2/FA-0034-2
FS-07-14	2008-2/FA-0034-2
FS-07-15	2008-2/FA-0034-2
FS-07-16	2008-2/FA-0034-2
FS-07-17	2008-2/FA-0034-2
FS-07-18	2008-2/FA-0034-2
FS-08-01	AUD-2009-2/FA-08-49-2
FS-08-02	AUD-2009-2/FA-08-49-2
FS-08-03	AUD-2009-2/FA-08-49-2
FS-09-01	AUD-2010-2/FA-09-64-2
FS-09-02	AUD-2010-2/FA-09-64-2
FS-09-03	AUD-2010-2/FA-09-64-2
FS-09-04	AUD-2010-2/FA-09-64-2
FS-09-05	AUD-2010-2/FA-09-64-2
FS-09-06	AUD-2010-2/FA-09-64-2
FS-09-07	AUD-2010-2/FA-09-64-2
FS-09-08	AUD-2010-2/FA-09-64-2
FS-09-09	AUD-2010-2/FA-09-64-2
FS-09-10	AUD-2010-2/FA-09-64-2
FS-09-11	AUD-2010-2/FA-09-64-2
FS-09-12	AUD-2010-2/FA-09-64-2
FS-09-13	AUD-2010-2/FA-09-64-2
FS-09-14	AUD-2010-2/FA-09-64-2
FS-09-15	AUD-2010-2/FA-09-64-2
FS-09-16	AUD-2010-2/FA-09-64-2
FS-09-17	AUD-2010-2/FA-09-64-2
FS-09-18	AUD-2010-2/FA-09-64-2
FS-09-19	AUD-2010-2/FA-09-64-2
FS-09-20	AUD-2010-2/FA-09-64-2

EXHIBIT I - Status of Internal Control Report Recommendations

FY Ended September 30, 2010	
FS-10-01	AUD-2011-3/FA-10-69-2
FS-10-02	AUD-2011-3/FA-10-69-2
FS-10-03	AUD-2011-3/FA-10-69-2
FS-10-04	AUD-2011-3/FA-10-69-2
FS-10-05	AUD-2011-3/FA-10-69-2
FS-10-06	AUD-2011-3/FA-10-69-2

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2010 and 2009 Financial Statements

Audit Report AUD-2011-3 / FA-10-69-2

Section II

Management Comments



Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

Office of the Director

MEMORANDUM

November 8, 2010

To: Rebecca Anne Batts
Inspector General

From: Josh Gotbaum 
Director

Subject: Response to the Office of Inspector General's (OIG's) Draft
Report on Internal Control for FY 2010

Thank you for the opportunity to respond to the subject draft report. PBGC is committed to addressing the recommendations contained in this report and to remediating the associated material weakness. We agree with the 43 recommendations in the draft special report on internal control. Of these, 37 recommendations remain open from prior audit findings with which management has already agreed. We also agree with the six new recommendations.

We have provided our responses to each recommendation below, and we will be updating our corrective action plans in the near future. We will keep your office informed as we move forward.

Entity-wide Security Program Planning and Management

1. Recommendation: Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses. **(OIG Control Number FS-09-01)**

Response: Management agrees. To address this and other prior year findings, PBGC developed a CAP that is a three- to five-year holistic approach. The CAP project represented a collaborative effort of subject matter experts from across OIT. The resulting plan used NIST 800-53 as a framework.

The CAP has been broken into several process families to address the underlying, root causes of the findings. These recommendations will primarily be addressed as we rebuild our IT Security Program. We expect to make progress each year toward the overall CAP, while adjusting schedules as necessary. PBGC will be communicating the progress and

any schedule adjustments to OIG on a regular basis, providing transparency of the overall CAP.

2. Recommendation: Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. **(OIG Control Number FS-08-01)**

Response: Management agrees. Please see response to #1, above. In addition, please note that, as we rebuild our IT Security Program, the list of 65 common controls may change. If they do, we will document those changes to facilitate our work and to provide you with an audit trail.

3. Recommendation: Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control Number FS-09-02)**

Response: Management agrees. Please see the response to Recommendation 2, above.

4. Recommendation: Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies. **(OIG Control Number FS-09-03)**

Response: Management agrees. Please see response to Recommendation #1, above.

5. Recommendation: Complete the development and implementation of the redesign of PBGC's IT infrastructure and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control Number FS-09-04)**

Response: Management agrees. Please see the response to Recommendation #1, above.

6. Recommendation: Implement an effective review process to validate the completion of the certification and accreditation packages for all major applications and general support systems. The review should not be performed by an individual associated with the performance of the C&A or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control Number FS-08-02)**

Response: Management agrees. Please see response to Recommendation #1, above.

7. Recommendation: Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the C&A process. **(OIG Control Number FS-09-05)**

Response: Management agrees. Please see response to Recommendation #1, above.

8. Recommendation: Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the certification and review process. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control Number FS-09-06)**

Response: Management agrees. Please see response to Recommendation #1, above.

9. Recommendation: Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC OIT operations. **(OIG Control Number FS-09-07)**

Response: Management agrees. Please see the response to Recommendation #1, above.

10. Recommendation: Implement an independent and effective review process to validate the completion of C&A packages for all applications and general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control Number FS-08-03)**

Response: Management agrees. Please see response to Recommendation #1, above.

11. Recommendation: Implement robust and rigorous review procedures to verify that future contracts for the C&A of PBGC's systems clearly outline expectations and deliverables in the statement of work. **(OIG Control Number FS-09-08)**

Response: Management agrees. Please see response to Recommendation #1, above.

12. Recommendation: Implement a robust and rigorous quality review process to verify contractor C&A deliverables meet the requirements specified in the statement of work. **(OIG Control Number FS-09-09)**

Response: Management agrees. Please see the response to Recommendation #1, above.

13. Recommendation: Establish controls to ensure that contract staff tasked with the C&A of PBGC systems have the appropriate knowledge and background to accurately and comprehensively complete the C&A process. **(OIG Control Number FS-09-10)**

Response: Management agrees. Please see the response to Recommendation #1, above.

14. Recommendation: Implement a robust and rigorous process to verify compliance with PBGC's policy on contractor management throughout the C&A lifecycle. **(OIG Control Number FS-09-11)**

Response: Management agrees. Please see the response to Recommendation #1, above.

15. Recommendation: Develop and implement a process to enforce the dissemination and awareness of PBGC's security policies and procedures through adequate training. **(OIG Control Number FS-07-04)**

Response: Management agrees. We have already initiated steps to address this recommendation. We have engaged in a Line of Business offering by the U.S. Office of Personnel Management (OPM) to promote information security and privacy awareness. We plan to implement computer-based training in FY 2011, which will enable automated tracking and reporting on who has received training. In addition, we are updating our policies and procedures to reflect new NIST guidance in this area. Moreover, we are enhancing the information security and awareness training program to provide role-based training where it is needed.

16. Recommendation: Establish, document, and publish measurable services that OIT provides to the Corporation, that are acceptable to all information system owners. **(OIG Control Number FS-07-06)**

Response: Management agrees. Please see response to Recommendation #1, above.

17. Recommendation: Develop and implement an immediate plan of action to address the potential security risk posed by locating the Security Operations Center outside of the US. **(OIG Control # FS-10-01)**

Response: Management agrees. Given the immediacy of the recommendation, management analyzed the situation and concluded that no significant additional risk is posed to the PLUS system that PBGC uses. Results of this analysis and conclusions are documented with the Security Plan for PLUS. Management will be pleased to discuss this further with OIG.

18. Recommendation: Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and FISMA. **(OIG Control # FS-10-02)**

Response: Management agrees. Management will review the existing contract with State Street Corporation to ensure that the contractor is required to be FISMA compliant.

19. Recommendation: Develop and implement an ISA and MOU with external organizations whose systems connect to PBGC's Consolidated Financial System (CFS). **(OIG Control # FS-10-02)**

Response: Management agrees with developing and implementing the appropriate, relevant agreements with external organizations whose systems connect with PBGC.

Access Controls and Configuration Management

20. Recommendation: Develop and implement procedures and processes for the consistent implementation of common configuration management controls to minimize security weaknesses in general support systems. **(OIG Control Number FS-07-07)**

Response: Management agrees. Please see response to Recommendation #1, above.

21. Recommendation: Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control Number FS-09-12)**

Response: Management agrees. Please see the response to Recommendation #1, above.

22. Recommendation: Establish baseline configuration standards for all of PBGC's systems. **(OIG Control Number FS-09-13)**

Response: Management agrees. Please see response to Recommendation #1, above.

23. Recommendation: Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control Number FS-09-14)**

Response: Management agrees. Please see response to Recommendation #1, above.

24. Recommendation: Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance. **(OIG Control Number FS-09-15)**

Response: Management agrees. Please see response to Recommendation #1, above.

25. Recommendation: Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **OIG Control Number FS-09-16)**

Response: Management agrees. Please see response to Recommendation #1, above.

26. Recommendation: Continue to remove unnecessary user and/or generic accounts. (OIG Control Number FS-07-08)

Response: Management agrees. Please see response to Recommendation #1, above.

27. Recommendation: Consistently implement controls to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. (OIG Control Number FS-07-09)

Response: Management agrees. Please see response to Recommendation #1, above.

28. Recommendation: Assess the risk associated with lacking segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. (OIG Control Number FS-09-17)

Response: Management agrees. Please see response to Recommendation #1, above.

29. Recommendation: Appropriately restrict developers' access to production environment to only temporary emergency access. (OIG Control Number FS-07-10)

Response: Management agrees. Please see response to Recommendation #1, above.

30. Recommendation: Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed. (OIG Control Number FS-09-18)

Response: Management agrees. Please see response to Recommendation #1, above.

31. Recommendation: Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications are in compliance with the IAH. (OIG Control Number FS-07-11)

Response: Management agrees. Please see response to Recommendation #1, above.

32. Recommendation: Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. (OIG Control Number FS-09-19)

Response: Management agrees. Please see response to Recommendation #1, above.

33. Recommendation: For the remaining systems, apply controls to lock out and remove inactive and dormant accounts after a specified period in accordance with the IAH. (OIG Control Number FS-07-12)

Response: Management agrees. Please see response to Recommendation #1, above.

34. Recommendation: Complete the implementation of the recertification process for all user and system accounts. Continue to perform annual recertification and include all PBGC's accounts (e.g. user, generic, service, and systems accounts) for general support systems and major applications. (OIG Control Number FS-07-13)

Response: Management agrees. Please see response to Recommendation #1, above.

35. Recommendation: Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. (OIG Control Number FS-07-14)

Response: Management agrees. Please see response to Recommendation #1, above.

36. Recommendation: Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. (OIG Control Number FS-09-20)

Response: Management agrees. Please see response to Recommendation #1, above.

37. Recommendation: Ensure that adequate documentation of access authorization is maintained by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. (OIG Control Number FS-07-15)

Response: Management agrees. Please see response to Recommendation #1, above.

38. Recommendation: Update and enforce directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. (OIG Control Number FS-07-16)

Response: Management agrees. PBGC Directive PM-05-1, *Entrance on Duty and Separation Procedures for Federal and Contract Employees* was updated and disseminated to PBGC Federal and Contract employees on October 19, 2010. This update enhances Internal Controls for the tracking of PBGC Contractors and reflects a more aggressive strategy for the tracking of Contractors at PBGC. The Internal Controls establishes accountability to the Contracting Officer's Technical Representative for the timely entrance on duty and separation of Contractors, as well as the documentation of their tenure at PBGC.

39. Recommendation: Implement a logging and monitoring process for application security related events and critical system modifications (e.g. CFS, PAS, TAS, PRISM, and IPVFB). **(OIG Control Number FS-07-17)**

Response: Management agrees. Please see response to Recommendation #1, above.

40. Recommendation: Replace the Citrix MetaFrame presentation server. **(OIG Control #FS-10-04)**

Response: Management agrees. PBGC will work with its paying agent to replace Citrix or come up with an interim solution until PLUS Web is deployed in 2011. PBGC will also consider including this in the boundary when future C&A's are completed.

41. Recommendation: Include the application virtualization/application delivery product used by the benefits payments service provider to access the PLUS application in the system boundary. **(OIG Control #FS-10-05)**

Response: Management agrees. Please see response to Recommendation #40, above.

42. Recommendation: Configure TeamConnect to ensure the integrity of the nightly premium output batch file error log. **(OIG Control #FS-10-06)**

Response: Management agrees.

Integrated Financial Management Systems

43. Recommendation: PBGC needs to develop and execute a plan to integrate its financial management systems in accordance with OMB Circular A-127. **(OIG Control Number FS-07-18)**

Response: Management agrees and appreciates the OIG's acknowledgement of PBGC's significant accomplishments to date. During FY 2010, the Financial Operations Department (FOD); Office of Information Technology and other PBGC Departments continued to follow through with PBGC's Corrective Action Plan (CAP) in several areas, as discussed below.

First, PBGC completed segment architectures for all segments containing financial management system functions, including the Consolidated Financial System (CFS); Premium Accounting; Benefits Administration; Procurement; and Budget. Moreover, the FOD has prepared and submitted to the Office of Management and Budget (OMB) Exhibit 300s for CFS and Premium Accounting that provide detailed plans for development, modernization, and enhancement efforts that are geared toward integrating the financial management systems. We believe the high level segment architectures, along with the more prescriptive Exhibit 300s constitute a solid roadmap to address this recommendation.

Secondly, the FOD implemented significant enhancements and technology modernization efforts to the Premium Accounting System (PAS) during FY 2010. The successful completion of this key modernization effort is a major milestone in PBGC's long term plan to replace and integrate its premium system. The PAS modernization effort provided major functional and technical changes in the areas of: (1) PPA Legislative changes; (2) upgrade of the Letter Generation Services to eALG; (3) improvements to the DOL Form 5500 interface; (4) Plan Genealogy Tracking and Reporting; and (5) database migration from Oracle 8i to 10g.

Going forward, PBGC has already planned future improvements to its Premium System. In its FY 2012 budget submission, FOD requested the funding to complete its new premium system that is planned for implementation by November 2013. When completed, this effort will address a cornerstone of PBGC's financial management systems with a modern and integrated premium accounting system.

Third, the FOD started efforts in FY 2010 to implement a new Trust Accounting System (TAS). The TAS project is intended to replace existing technology (e.g. Trust Interface System, FY File, and Portfolio Accounting and Management System) with a comprehensive, modern, and integrated solution to account for and manage investments of trustee plans. The TAS effort is scheduled for completion no later than September 2012.

In FY 2010, the FOD also started to modernize the manual interface between the Consolidated Financial System (CFS) and the Comprizon Suite (Procurement System) that is scheduled to be implemented in FY 2011. When completed, this electronic interface should upload obligating documents from the Comprizon Suite to the CFS, thereby eliminating the need to manually record obligations, eliminating duplicate entry, and reducing the risk of inaccurate financial information.

Lastly, in FY 2011, FOD will be implementing electronic interfaces between the (1) CFS and FedTraveler (Travel Management System) and the (2) CFS and the Federal Personnel Payroll System (U.S. Department of Interior Payroll System). These interface efforts should complete integration of the remaining key applications that now interface manually with the CFS, thereby eliminating manual processes to record travel and payroll information, eliminating duplicate entry, and reducing the risk of inaccurate financial information. Also during FY 2011, the FOD will be implementing Electronic Invoicing to track and automatically route invoices for approval to increase the timeliness of processing vendor invoices for payment.

If you want to report or discuss confidentially any instance of misconduct, fraud, waste, abuse, or mismanagement, please contact the Office of Inspector General.

Telephone:
The Inspector General's HOTLINE
1-800-303-9737

The deaf or hard of hearing, dial FRS (800) 877-8339 and give the Hotline number to the relay operator.

Web:
<http://oig.pbgc.gov/investigation/details.html>

Or Write:
Pension Benefit Guaranty Corporation
Office of Inspector General
PO Box 34177
Washington, DC 20043-4177